IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application of:		)
Inventors:	Guy Eden	)
Serial No.:	09/944,684	) ATTORNEY FILE NO. SLA1086
Filed:	August 31, 2001	)
		) Customer No.: 55,286
Title:	SYSTEM AND METHOD FOR USING A PROFILE TO ENCRYPT DOCUMENTS IN A DIGITAL SCANNER	) Examiner: Ha, Leynna A.) Group Art: 2135) Confirmation No.: 2139

Board of Patent Appeals and Interferences
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

BRIEF ON APPEAL

This is an appeal from the rejection by Examiner Leynna A. Ha, Group Art Unit 2135, of claims 1-2, 4-14, and 16-27 as set forth in the CLAIMS APPENDIX, all claims in the application.

REAL PARTY IN INTEREST

The real party in interest is Sharp Laboratories of America, Inc., as assignee of the present application by an Assignment in the United States Patent Office, with a recordation date of August 31, 2001, at Reel 012147, Frame 0324.

RELATED APPEALS AND INTERFERENCES

None.

STATUS OF THE CLAIMS

Claims 3 and 15 have been canceled.

Claims 1-2, 4-14, and 16-27 are in the application.

Claims 1-2, 4-14, and 16-27 are rejected.

Claims 1-2, 4-14, and 16-27 are appealed.

STATUS OF AMENDMENTS

Amendments to the claims were made in a paper mailed on October 18, 2005. These claim amendments have been entered.

SUMMARY OF CLAIMED SUBJECT MATTER

Conventionally, scanners send binary images or electronic documents via unsecured networks, for example, the Internet or a local area network (LAN). As used herein, a scanner may be a digital copier or multifunctional peripheral (MFP) that employs multiple functions, such as scanning, copying, printing, and faxing. If security is desired, a user may transmit a scanned document to their own terminal for encryption, via a local network (e.g., a LAN). The encryption algorithm is established

at the sender's terminal, and the encrypted document can be safely transmitted to a destination via a non-trusted network (e.g., as an email attachment sent via the Internet). This constitutes a cumbersome three-stage process. Further, this three-stage process assumes that the local network (between the scanner and terminal) is secure. However, an electronic eavesdropper may reside between the scanner and the user's terminal, who can capture a document before it is encrypted.

As described in the specification at line 3 of page 15, to line 14, and depicted in Fig. 5, claim 1 recites a process for securely transmitting a document from a scanner. Step 502 creates a profile with an address field and an encryption field, and Step 504 stores the profile in a directory. Subsequently, the method accepts a physical medium document, and in Step 506 a profile is selected. The document is scanned in Step 508. Step 510 encrypts the document is response to the encryption field of the selected profile. In Step 512, the encrypted document is sent to a destination responsive to the address field of the selected profile. As compared to the above-mentioned conventional process, the method of claim 1 is both simpler and safer, in that the document need not be transmitted to the user's terminal for encryption.

Claim 13 also describes a method for securely transmitting a document from a scanner. Claim 13 is also supported by Fig. 5, and lines 3-14 on page 15 of the specification. The method stores a profile in a directory associated with the scanner. The profile includes an address field and an encryption field (Steps 502, 503, and 504). Step 506 selects a profile. Step 508 scans a document. Step 510 encrypts the scanned document in response to the encryption field of the selected profile. Step

512 sends the encrypted document to a destination responsive to the address field of the selected profile.

Claim 27 describes another method for securely transmitting a document from a scanner. Claim 27 is also supported by Fig. 5, and lines 3-14 on page 15 of the specification. The method cross-references an address field to an encryption field (Step 502) and stores the cross-referenced fields in a directory (Step 504). Step 506a selects an address from the directory. The method accepts a physical medium document and Step 508 scans the document. Step 510 encrypts the scanned document using the cross-referenced encryption field. Step 512 sends the encrypted document to a destination using the selected address field.

As described in the specification at page 6, line 23, through page 7, line 25, and depicted in Figs. 1 and 2, the invention of claim 14 is a scanner with a secure document transmission system 100. The system 100 includes a profile directory 102 with a user interface 104 for selecting a profile. Fig. 2 depicts some exemplary profiles. Each profile includes an address field (e.g., destination), and an encryption field (e.g., encryption key). Returning to Fig. 1, a document scanner 106 accepts a physical medium document 108, and creates a scanned document that is encrypted in response to the encryption field of the selected profile. The encrypted document is sent via network interface 110 to a destination responsive to the address field of the selected profile.

As described in the specification at page 6, line 23, through page 2, line 25, and depicted in Figs. 1 and 2, the invention of claim 26 is a scanner with a secure document transmission system 100. The system 100 includes a profile directory 102 with a user interface 104 for selecting an address field that is cross-referenced to an encryption filed. A

document scanner 106 accepts a physical medium document 108, and creates a scanned document that is encrypted in response to the cross-referenced encryption field. The encrypted document is sent via network interface 110 to a destination responsive to the selected address field.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Whether claims 1-2, 4-9, 11-14, 16-23, and 25-27 are unpatentable under 35 U.S.C. 103(a) with respect to Seder et al. ("Seder"; US 6,694,043).

2. Whether claims 10 and 23 are unpatentable under 35 U.S.C. 103(a) with respect to Seder in view of Hind et al., ("Hind"; US 6,980,660).

ARGUMENT

1. The rejection of claims 1-2, 4-9, 11-14, 16-23, and 25-27 as unpatentable under 35 U.S.C. 103(a) with respect to Seder et al. ("Seder"; US 6,694,043).

With respect to claims 1, 13, 14, and 26-27 the Office Action states that Seder describes a profile, a profile address field, a profile encryption field, the storing of profiles in a directory, the selection and association of a profile with a scanned document, and the transmission of the scanned document responsive to the profile address and encryption fields.

An invention is unpatentable if the differences between it and the prior art would have been obvious at the time of the invention. As

stated in MPEP § 2143, there are three requirements to establish a *prima facie* case of obviousness.

> First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck* 947 F.2d 488, 20 USPQ2d, 1438 (Fed. Cir. 1991).

Generally, Seder describes a stenanographic encoding system which creates a watermark that is (invisibly) superimposed on a document. Upon photographing the document, the watermark can be detected. Once identified, the watermark may be used to prompt an action, such as identifying the file name of the document (col. 1, ln. 30-54).

In contrast, the invention of claims 1, 13-14, and 26-27 describes a directory of profiles. Each profile includes an address field and an encryption field. After scanning a document, a user selects a profile. The selection of a profile from the directory automatically sends the scanned document to a particular address, using a particular form of encoding, as specified in the fields of the selected profile.

Seder appears to describe none of the elements recited in the Applicant's independent claims. Claim 1 for example, recites a profile with an address field and an encryption field. The Office Action states that Seder describes a profile at col. 2, ln. 63-67. However, the cited portion of Seder discloses the "payload" associated with a watermark. Information may be literally encoded in the payload (col. 2, ln. 57-58), or

the payload can be used as an index to another repository where additional information (metadata) associated with the document may be stored as a "record". Seder's record identifies a particular document in storage. The Applicant's profile is not used to identify a document, or to access a stored document.

In the ***Response to Arguments*** Section of the Final Office Action (page 17) states that Seder's record can reasonable be interpreted to be a text file with an address field and encryption field, citing col. 2, ln. 16-23 and 52-67. However, as noted above, the cited sections of the Seder disclosure merely describes a "watermark" that acts as an index to data repository where auxiliary information is stored. The cited sections are presented below:

Column 2, lines 16-23:

> In accordance with one embodiment of the invention, a steganographic watermark is added to a document at the time of printing. The printing may be done by a standard office printer (e.g., ink-jet, laser, etc.), or a large clustered on-demand document printer. Each document copy thus contains a mark that can be used to uniquely identify the document. Such marks can be registered in a database and used to link to information about the document.
>
> ....

Column 2, lines 52-67:

> (The length of the payload depends on the application. In some cases, a single bit payload will suffice (e.g., it may serve as a flag to convey a single item of status information about a document--such as confidential, do-not-copy, draft, etc.) Or several such flags may be conveyed by a relatively short payload. Certain textual or numeric information may be literally encoded by the payload, such as the date and time the document was printed (e.g., a 24-bit number representing the number of elapsed minutes since

> Jan. 1, 2000). The foregoing are examples of direct data encoding. Indirect data encoding, such as the 32 bit identifier cited above, uses the payload as an index into another data repository in which large collections of data can be stored. This collection (sometimes called a "record") may include meta-data associated with the document, such as date, author, size, keywords, file name and storage address, footnotes or other annotations, checksum, etc. In one particular embodiment, identifiers are issued sequentially, with each document thereby assigned a unique identifier.)

As can be understood from reading the above-cited section, Seder's index or watermark does not match the Applicant's definition of an address field. Further, the cited section is absolutely silent with respect to the subject of encryption.

The Office Action states that a profile address field is disclosed at col. 3, ln. 52-53. The cited section of Seder discloses an embodiment where a stored document is presented on a user screen as a response to identifying a watermark (col. 3, ln. 39-44). Seder notes that the addresses of stored documents may change, and describes a software program (daemon) that monitors the movements of documents in a database. The Applicant respectfully submits that this document-tracking daemon is not associated with the watermark or the watermark payload. Therefore, the software daemon cannot be considered a "profile address field". Further, the Applicant notes that a profile address field, as recited in the Applicant's claims and described in the specification, is a destination to which a document is sent, not an address from which a stored document is retrieved.

The ***Response to Arguments*** Section (page 17) states that "the profile address field is not the address for sending. The address field cited in the rejection refers to the claims "the creating computer text files, called profiles, in a directory of a scanner device..." In response, the

Applicant's claims, specification, and drawings are consistently clear in stating that an address field is a destination to which an encrypted document is sent. The limitations associated with the recited address field cannot be ignored.

The Office Action states that Seder discloses a profile encryption field at col. 6, ln. 18-24. Seder states that printed documents may be encrypted, and the encryption key created as a watermark on the document. In the cited section of text, however, Seder merely states that printed documents may point to encryption keys that permit electronic access to unrelated documents.

The ***Response to Arguments*** Section (page 18) states that the claimed encryption field "can broadly be given in light of the area or parameter of the record that indicates the encryption information." In response, the Applicant notes that an encryption field is not being broadly claimed. Rather, the recited encryption field includes the limitations of being embedded in a profile, associated with an address field, and temporarily linked with a scanned document. Seder does not disclose these limitations, and the Office Action fails to even attempt to build a case that an expert would find these limitation obvious in light of Seder.

The Final Office Action states that Seder describes the sending of an encrypted document to a destination in response to a profile address field. At col. 4, ln. 28-33, Seder describes a hypertext link embedded in a document. A hypertext link is not a profile address field. That is, Seder's document is not sent to the hypertext link address. Seder describes an option of encoding a key in a watermark, to retrieve an encrypted electronic document (col. 6, ln. 8-12). Again, a watermark is not

a profile, and creating a watermark decryption key is not the same process as using a profile to encrypt a scanned document prior to transmission.

To summarize, Seder discloses a watermark associated with a printer document, which may point to a record of document information record, while the Applicant recites a profile which may be selectively associated with a scanned document. Seder's system can be used to locate a stored document in a database memory, while the Applicant's profile address field is used to send a scanned document to an address. Seder's system can be used to decrypt a printed document or to gain access to unrelated documents, while the Applicant's encryption field is used to encrypt a scanned document prior to transmission.

The Applicant respectfully requests that the recited claim elements of a "profile", "profile address field", and "profile encryption field" be interpreted as they are defined in the claims. In the event of ambiguity, these claim terms should be interpreted as they are defined in the specification.

The current consensus of the CAFC is that the claims are to be interpreted in light of the supporting specification, as described in *Phillips v. AWH Corp.* No. 03-1269 (Fed. Cir. 7/12/2005). In this decision, the Court stated:

"Importantly, the person of ordinary skill in the art is deemed to read the claim term not only in the context of the particular claim in which the disputed term appears, but in the context of the entire patent, including the specification. This court explained that point well in Multiform Desiccants, Inc. v. Medzam, Ltd., 133 F.3d 1473, 1477 (Fed. Cir. 1998):

> It is the person of ordinary skill in the field of the invention through whose eyes the claims are construed. Such person is deemed to read the words used in the patent documents with an understanding of their meaning in the field, and to have knowledge of any special meaning and usage in the field. The inventor's words that are used to describe the invention-the inventor's lexicography-must be understood and interpreted by the court as they would be understood and interpreted by a person in that field of technology. Thus the court starts the decisionmaking process by reviewing the same resources as would that person, viz., the patent specification and the prosecution history."

The profile, with address and encryption fields, is discussed in the Applicant's specification at page 7, lines 11, through page 3, line 20, and shown in Fig. 2. Seder's use of watermarks and records does not disclose the use of a profile, profile address field, or profile encryption field, as defined in the Applicant's claims.

With respect to the *first prima* facie requirement, the Office Action fails to provide any motivation to suggest that a person skilled in the art would have found it obvious to modify Seder's system in such a manner as to yield the claimed invention. In fact, the Office Action merely states that, "it would have been obvious for a person of ordinary skill in the art that the electronic document as taught by Seder has been the scanned document because the equipment processing in Seder is operable to receive scanned documents."

The legal concept of *prima facie* obviousness is a procedural tool of examination which applies broadly to all arts. It allocates who has the burden of going forward with production of evidence in each step of the examination process. See *In re Rinehart*, 531 F.2d 1048, 189 USPQ 143 (CCPA 1976); *In re Linter*, 458 F.2d 1013, 173 USPQ 560 (CCPA 1972); *In re Saunders*, 444 F.2d 599, 170 USPQ 213 (CCPA 1971); *In re*

Tiffin, 443 F.2d 394, 170 USPQ 88 (CCPA 1971), *amended*, 448 F.2d 791, 171 USPQ 294 (CCPA 1971); *In re Warner*, 379 F.2d 1011, 154 USPQ 173 (CCPA 1967), *cert. denied*, 389 U.S. 1057 (1968).

The CAFC has consistently found over the years that a *prima facie* case for obvious must be based upon a detailed analysis of how and why an expert could excerpt known art to make modifications to a cited prior art reference. A *prima facie* case cannot be supported by the simple statement that the Applicant's invention is made obvious merely because Seder's processing equipment may receive scanned documents.

In other words, the examiner must show reasons that the skilled artisan, confronted with the same problems as the inventor and with no knowledge of the claimed invention, would select the elements from the cited prior art reference for combination in the manner claimed." *In re Rouffet*, 47 USPQ2d 1453, 1457-1458 (1998).

Returning to the first *prima facie* requirement, Seder's system is used for a totally different purpose than the Applicant's invention. Seder uses watermarks, identified on a printed document, or indexed records to identify a stored electronic document. The Office Action has failed to suggest, in even the most general way, how the identification of watermarks or indexed records points to a system which uses a profile to streamline the transmission of a scanned document. With respect to the second *prima facie* requirement, the Office Action provides absolutely no evidence of an expectation of success.

With respect to the third *prima facie* requirement, Seder does not explicitly suggest every limitation of the claimed invention. As noted in detail above, Seder does not disclose a profile, a profile address field, a profile encryption field, the selection of a profile, the transmission of a

scanned document in response to a selected profile, the transmission to the destination associated with the profile address field, or the encryption of the transmission in response to the profile encryption field. Since Seder does not explicitly describe or suggest these claim elements, he cannot be said to make obvious all the limitations of independent claims 1, 13-14, and 26-27. Claims 2, 4-9, and 11-12, dependent from claim 1, and claims 16-23 and 25, dependent from claim 14, enjoy the same distinctions from the cited prior art reference.

The Affidavit of Budd Levin (see Evidence Appendix) was presented with the Office Action response mailed on September 27, 2006. To summarize, Mr. Levin states that Seder discloses a system that uses a "watermark" for identifying or tagging a printed document. In one embodiment, the watermark can be used as a pointer, to access auxiliary information (a record) concerning the document.

Mr. Levin states that a one-to-one relationship is created between a record and a document. The Applicant's profile, which the Examiner alleges reads on Seder's record, is not associated with a document. Rather, the Applicant's profile is a set of processing instructions. Once the processes (encryption/transmission) are completed, the temporary linkage between the profile and document is broken.

More particularly, the address field cited by the examiner is a system for managing the linkage between records and documents, in case the location of the record is moved. The Applicant's address field is not used for locating a document or a profile in a database.

The Final Office Action states Mr. Levin's affidavit is an affirmation that he has never seen the claimed subject matter, and is not relevant to the issue of nonobviousness, citing MPEP 716. The Office

Action states that Mr. Levin's knowledge "fails to provide evidence toward any prior art teaching of such affirmation. The examiner's prior art (Seder and Hind) rejection reads on the claimed invention. Thus, the prior art of record overcomes Mr. Burtons (sic) personal beliefs or knowledge."

However, MPEP 716.01(c) III states that "(a)lthough an affiant's or declarant's opinion on the ultimate legal issue is not evidence in the case, "some weight ought to be given to a persuasively supported statement of one skilled in the art on what was not obvious to him." 385 F.2d, 485, 155 USPQ, 524.

The Examiner's entire argument for modifying Seder, in a manner that make the claimed invention obvious, is based upon the one-line statement that "it would have been obvious for a person of ordinary skill in the art that the electronic document as taught by Seder has been the scanned document because the equipment processing in Seder is operable to receive scanned documents." The affidavit of Mr. Levin is presented to provide a more accurate portrayal of the Seder reference, than the interpretation presented in the Office Action. The affidavit is also a statement by a person with years of experience in the art, that the claimed invention is not obvious in light of the prior art.

2. The Rejection of claims 10 and 23 as unpatentable under 35 U.S.C. 103(a) with respect to Seder in view of Hind et al., ("Hind"; US 6,980,660).

In Section 5 of the Final Office Action claims 10 and 23 have been rejected under 35 U.S.C. 103(a) as being unpatentable with respect to Seder in view of Hind. The Office Action acknowledges that Seder fails

to disclose certification authority, but states that it would have been obvious to include the public key encryption of Seder with the certificate authority taught by Hind.

Hind describes a method for encrypting wireless communications. Hind does not disclose the use of profiles, profile address fields, profile encryption fields, or the sending of scanned documents in response to selecting a profile from a directory. As noted above, the Office Action has not made a *prima facie* case to support the rejection of claims 1 and 14 as obvious with respect to Seder. Therefore, even if Hind can be combined with Seder, that combination still does not suggest or make explicit all the limitations of independent claims 1 and 14. Claims 10 and 23 enjoy the same distinctions over the prior art references.

SUMMARY AND CONCLUSION

It is submitted that for the reasons pointed out above, the claims in the present application clearly and patentably distinguish over the cited references. Accordingly, the Examiner should be reversed and ordered to pass the case to issue.

The fee for filing this Appeal Brief is enclosed. Authorization is given to charge any deficit or credit any excess to Deposit Account No. 502,033.

Respectfully submitted,

Date: 12/11/2006

Gerald Maliszewski
Registration No. 38,054

Customer Number 55,286
P.O. Box 270829
San Diego, CA 92198-2829
Telephone: (858) 451-9950
Facsimile: (858) 451-9869
gerry@ipatentit.net

TABLE OF CONTENTS

CLAIMS APPENDIX

1. (Previously Presented) In a digital scanner, a method for secure document transmission, the method comprising:

creating computer text files, called profiles, each profile having an address field and an encryption field;

storing the profiles in a directory;

at a scanner device user interface, selecting a profile from the directory;

accepting a physical medium document;

scanning the document;

encrypting the scanned document in response to the encryption field of the selected profile; and,

sending the encrypted document to a destination in response to the address field of the selected profile.

2. (Previously Presented) The method of claim 1 wherein sending the encrypted document to the destination includes sending the encrypted document to a network-connected destination in response to the address field of the selected profile.

3. Canceled

4. (Previously Presented) The method of claim 1 further comprising:

assigning each profile to a corresponding destination; and,

wherein selecting a profile includes:

selecting a destination; and,

using the profile assigned to the selected destination.

5. (Previously Presented) The method of claim 1 wherein selecting a profile includes selecting a profile having an address selected from the group including email addresses and file transfer protocol (FTP) addresses.

6. (Previously Presented) The method of claim 1 wherein selecting a profile includes selecting a profile having an encryption field selected from the group including symmetric and asymmetric (public) keys.

7. (Original) The method of claim 6 wherein selecting a profile includes selecting a profile having an asymmetric key; and,

wherein creating profiles includes storing public keys in the created profiles.

8. (Original) The method of claim 6 wherein selecting a profile includes selecting a profile having a symmetric key; and,

wherein creating profiles includes storing symmetric keys in the created profiles.

9. (Previously Presented) The method of claim 1 wherein creating profiles includes creating profiles for a plurality of user groups;

the method further comprising:

generating a plurality of passwords for the corresponding plurality of user groups; and,

wherein storing the profiles in a directory includes storing profiles in a profile directory, in response to the generated password.

10. (Previously Presented) The method of claim 1 wherein selecting a profile includes selecting a profile having a link to a certification authority storing a public key; and,

wherein encrypting the document using the encryption field from the selected profile includes using the public key signed by the certification authority to encrypt the document.

11. (Original) The method of claim 7 wherein encrypting the document using the encryption field from the selected profile includes:

generating a random session key;

encrypting the document with the session key using a symmetric algorithm;

encrypting the session key with an asymmetric algorithm using the selected profile public key; and,

wherein sending the encrypted document to the address from the selected profile includes sending the encrypted session key.

12. (Original) The method of claim 6 wherein creating profiles includes creating a profile with a plurality of addresses and a corresponding plurality of public keys;

wherein encrypting the document includes generating a single encrypted document using an asymmetric algorithm; and,

wherein sending the encrypted document includes sending the single encrypted document to each of the plurality of addresses in the profile.

13. (Previously Presented) In a digital scanner, a method for secure document transmission, the method comprising:

storing computer text files, called profiles, in a directory of a scanner device, each profile having an address field and an encryption field;

at a user interface associated with the scanner device, selecting a profile from the directory;

scanning a document;

encrypting the scanned document in response to the encryption field of the selected profile; and,

sending the encrypted document from the scanner device, to a network-connected destination, in response to the address field of the selected profile.

14. (Previously Presented) A digital scanner secure document transmission system, the system comprising:

a profile directory having a user interface for selecting computer text files, called profiles, each profile including an encryption field and an address field;

a document scanner to accept physical medium documents, create scanned documents, and encrypt the scanned documents in response to selected profile encryption fields; and,

a network interface for transmitting the encrypted documents to a destination in response to the profile address field.

15. Canceled

16. (Previously Presented) The system of claim 14 further comprising:

a memory for storing the profiles; and,

wherein the profile directory has an interface for creating profiles having an address field and an encryption field;

17. (Original) The system of claim 16 wherein the profile directory has an interface for accepting destinations and assigning each profile to a corresponding destination; and,

wherein profiles are selected from the profile directory in response to entering the destination.

18. (Original) The system of claim 16 wherein the profile directory supplies selected profiles having an address selected from the group including email addresses and file transfer protocol (FTP) addresses.

19. (Original) The system of claim 16 wherein the profile directory supplies selected profiles having an encryption field

selected from the group including symmetric and asymmetric (public) keys.

20. (Original) The system of claim 19 wherein the profile directory supplies selected profiles having an asymmetric key; and,

wherein the memory stores the public keys corresponding to each profile.

21. (Original) The system of claim 19 wherein the profile directory supplies selected profiles having a symmetric key; and,

wherein the memory stores the symmetric keys corresponding to each profile.

22. (Original) The system of claim 16 wherein the profile directory has an interface for generating passwords, the profile directory creating profiles for a plurality of user groups in response to the generated passwords.

23. (Original) The system of claim 16 further comprising:

a certification authority storing public keys;

wherein the profile directory supplies a selected profile having a link to the certification authority;

wherein the network interface negotiates with the certification authority for a public key corresponding to the selected profile; and,

wherein the document scanner uses the public key signed by the certification authority to encrypt the document.

24. (Original) The system of claim 20 wherein the document scanner generates a random session key and encrypts the document with the session key using a symmetric algorithm;

wherein the document scanner encrypts the session key with an asymmetric algorithm using the selected profile public key; and,

wherein the network interface transmits the encrypted session key with the encrypted document.

25. (Original) The system of claim 19 wherein the profile directory supplies a selected profile with a plurality of addresses and a corresponding plurality of public keys;

wherein the document scanner encrypts the document into a single encrypted document using an asymmetric algorithm; and,

wherein the network interface sends the single encrypted document to each of the plurality of addresses in the selected profile.

26. (Previously Presented) A digital scanner secure document transmission system, the system comprising:

a directory having a user interface for selecting an address field cross-referenced to an encryption field;

a document scanner to accept physical medium document, create a scanned document, and encrypt the scanned document using the cross-referenced encryption field; and,

a network interface for transmitting the encrypted document to a destination using the selected address field.

27. (Previously Presented) In a digital scanner, a method for secure document transmission, the method comprising:

cross-referencing an address field to an encryption field;

storing the cross-referenced fields in a directory;

at a scanner device user interface, selecting an address from the directory;

accepting a physical medium document;

scanning the document;

encrypting the scanned document using the cross-referenced encryption field; and,

sending the encrypted document to a destination using the selected address field.

EVIDENCE APPENDIX

DECLARATION OF BURTON L. LEVIN UNDER 37 CFR 1.132

I, Burton Levin, hereby declare as follows:

1. My residence address is 3088 Rosemary Lane, Lake Oswego, OR 97034.

2. Since March 31, 1999 I have been employed by Sharp Laboratories of America (SLA), Inc., 5700 N.W. Pacific Rim Boulevard, Camas, Washington 98607. From March 31, 1998 to March 30, 1999, I was a contractor, working for Sharp Laboratories as a Program Manager. My title is Senior Program Manager. My responsibilities include development of firmware and software related to image processing, including printer drivers, color imaging, scanner and copier firmware.

3. My educational background includes a BS, Mathematics and Physics, University of Illinois, and a Master of Science/Computer Science from West Coast University.

4. Prior to my employment with SLA, I worked at Atlas Telecom where I was Director of Engineering. Prior to working at Atlas Telecom, I was Vice President of Engineering at Interconnectix, Portland Oregon. My background includes the design and development of complex hardware, firmware, and software products. I have several patents for inventions in VLSI design, memory architecture, and software in a diversity of applications spanning the last 24 years. I have further developed IP in divers areas, such as, for image handling and software/hardware appliances to help the visually handicapped in their home and business environments.

5. I have read the claims and relevant portions of the specification for the patent application at issue, Serial No. 09/944,684, entitled "System and Method for Using

a Profile to Encrypt Documents in a Digital Scanner", invented by Guy Eden. I have also read the Office Action of June 29, 2006, where the Applicant's claims have been rejected as obvious. I have read the relevant sections from the three prior art references: Seder et al. and Hind et al.

5. The primary reference upon which the examiner relies is Seder et al. It is my opinion that the Seder et al. reference cannot be said the make the Applicant's claims obvious. First, the entire point and purpose of the Seder et al. invention is different than the purpose stated in the applicant's independent claims (claims 1, 13, 14, 26, and 27). Second, the components of the Seder et al. system are completely different than those described in the applicant's claims. For this reason, I do not think that a person of skill in the field of scanning and printing imaging device driver software, such as myself, could possibly derive the applicant's claimed invention by "tinkering" with the Seder et al. design. Even if the Hind et al. invention is merged with Seder et al, that merger still does not make obvious the use of the applicant's invention, or the components used to enable the invention described by the applicant's claims.

6. Seder et al. describes a process for tagging a printed document with an invisible watermark at the time of printing. The watermark is associated with a payload. The bigger the payload, the more information that can be loaded into the watermark, for identifying attributes of the document. Thus, the payload refers to the complexity of the watermark, and the watermark is a device for identifying or tagging a printed document. Seder et al. also states that the watermark payload can be used as a pointer to a "record", which includes more detailed information about the document.

The examiner refers to the record of Seder et al. as a profile, because both elements are files. However, I find this analysis flawed. On the most abstract level, each record of Seder et al. describes a particular stored document, and there is a one-to-one, fixed relationship between a record and document. The applicant's profile on the other hand, does not describe a document, and is not fixedly linked with a document. Rather, the applicant's profile is a set of processing instructions which are momentarily associated with a scanned document. In the present case, the processing instructions concern encryption and destination address. Once the processes are carried out, the linkage between the profile and scanned document is broken.

The examiner also describes the records of Seder et al. as having an address field and an encryption field. The so-called address field described by Seder et al. is a system for managing the address of the record in the database, in case the record is moved. Again, the correlation between record and profile cannot be maintained. While Seder et al. describes the location of record with a changing address, the applicant describes a field inside profile. This address field has nothing to do with locating the profile. Rather, the profile field is used as a scanned document destination.

The examiner writes that Seder et al. describe a profile encryption field in column 6 of the patent. However, column 6 describes some encryption processes that can be triggered in response to identifying a watermark on a printer document. Here, the examiner is attempting to equate a watermark with the applicant's profile. However, a printed watermark is clearly not a data file or text file. Therefore, a watermark cannot have a field of any kind.

7. In summary, Seder et al. describe a system that permits a user to identify and/or access a stored electronic document in a database, by first identifying a watermark on a printed version of the document. At the most abstract level, I do not see how such a system would suggest a system that momentarily links a profile with a scanned document, to automate the transmission and encryption processes. On the more detailed level, Seder et al. does not describe the applicant's profile, having address and encryption fields. So even if an expert were motivated to invent a system to perform the same function described in the applicant's claims, Seder et al. does not provide an expert with the "building blocks" needed to enable the applicant's claims.

8. The Hind et al. invention is presented to introduce details concerning encryption keys and certificate authority. Hind et al. describes an invention in the context of a wireless communications environment, and I am not certain that an expert in the scanning/printing field would look to the field of wireless communications for ideas. However, that point is not relevant, because even if the two inventions are merged, that merger cannot make the applicant's claims obvious. Again, at the most abstract level, neither of the two prior art patents suggests the purpose of the applicant's invention, and neither describes the components that would be needed to enable the applicant's invention.

9. I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and further that these statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United State Code and that such willful,

false statements may jeopardize the validity of the application on any patent issuing thereon.

Date: 27 Sept. 2006 Signed: Burton Levin

Burton (Budd) Levin

RELATED PROCEEDINGS APPENDIX

NONE